

All About NSA's and AT&T's Big Brother Machine, the Narus 6400

by [bewert](#)

Fri Apr 07, 2006 at 10:47:24 PM PDT

Earlier today we found out that the EFF had sued AT&T over their secret work with the NSA on surveillance of millions of US citizens without wiretaps. We learned that paragraph 65 of this complaint shows EFF is trying to turn it into a [nationwide Class Action suit covering all current and former customers \(any after 9/2001\) of AT&T](#). And we learned that a [retired AT&T technician had stepped forward and disclosed the installation of secret NSA spy equipment in the San Francisco trunk facility. As well as the belief that similar equipment is in place in Seattle, San Jose, Los Angeles and San Diego](#).

Specifically, this equipment was the Narus ST-6400, a machine that was capable of monitoring over 622 Mbits/second in real time in May, 2000, and capturing anything that hits its' semantic (i.e. the meaning of the content) triggers. The latest generation is called NarusInsight, **capable of monitoring 10 billion bits of data per second**.

Follow me over the jump and let's learn some more about the private company Narus, it's founder Ovi Cohen, and board member Bill Crowell. Shall we?

[bewert's diary](#) :: ::

Narus is a private company founded in 1997 by Ori Cohen, who had been in charge of technology development for VDONet, an early media streaming pioneer. It has venture funding from an all-star team of investors including JP Morgan Partners, Mayfield, NeoCarta, Presidio Venture Partners, Walden International, Intel, NTT Software and Sumisho Electronics.

Of note is that while [Hoover's company factsheet on Narus](#) continues to list Mr. Cohen as Chairman, while Narus's own website [listing of the Board of Directors](#) no longer mentions Mr. Cohen.

Prior to 9/11 Narus worked on building carrier-grade tools to analyze IP network traffic for billing purposes, to prevent what they term "revenue leakage". Post-9/11 they have continued down that path while adding more semantic monitoring abilities for surveillance purposes. They even brought in [former Deputy Director of the NSA William P. Crowell](#) as an addition to their Board of Directors. From the Press Release announcing this:

Crowell is an independent security consultant and holds several board positions with a variety of technology and technology-based security companies. Since 9/11, Crowell has served on the Defense Advanced Research Projects Agency (DARPA) Task Force on Terrorism and Deterrence, the National Research Council Committee on Science and Technology for Countering Terrorism and the Markle Foundation Task Force on National Security in the Information Age.

His past positions have included president and chief executive officer of Cylink, a leading provider of e-business security solutions, as well as a series of senior positions at the National Security Agency, including deputy director of operations and deputy director of the Agency. Crowell has served as chairman of the President's Export Council (PEC) Subcommittee on Encryption, which worked with the Administration, Congress and private industry to substantially loosen restrictions on the export of encryption products and technology.

"Narus has an impressive track record of working with tier-one carriers to keep their networks running safely, continuously and profitably," said William Crowell. "I look forward to helping Narus as they forge new strategic partnerships and continue to break new ground in the telecommunications industry."

So these guys (1) build hugely cool network monitoring devices and (2) are tied into US (at least) national security organizations at the highest levels. What are these hugely cool machines capable of?

From [the Key Features list of NarusInsight](#)

- Universal data collection from links, routers, soft switches, IDS/IPS, databases, etc. provides total network view across the world's largest IP networks.
- Normalization, Correlation, Aggregation and Analysis provide a comprehensive and detailed model of user, element, protocol, application and network behaviors, in real time.
- Seven 9s reliability from data collection to data processing and analysis.
- Industry-leading packet processing performance that supports network speeds of up to OC-192 at layer 4 and OC-48 at layer 7, enabling carriers to monitor traffic at either the edge of the network or at the core.
- Unsurpassed and limitless scalability to support the world's largest, most complex IP networks.
- Unparalleled flexibility -- NarusInsight's functionality can easily be configured to meet any specific customer requirement (Narus Software Developer Kit -SDK).
- Unparalleled extensibility -- **NarusInsight's functionality can easily be configured to feed a particular activity or IP service such as security, lawful intercept or even Skype detection and blocking.**

How powerful is this? **OC-192 carries about 10 gigabits of data per second. Ten billion bits per second, monitored in real-time.** That is stunning. This is one damned powerful machine, one of the most powerful I've ever heard of in 25 years in IT.

And what does it monitor while looking at this 10 billion bits of IP data per second? First lets take a look at what the network model is, the **OSI model of seven layers**. NarusInsight focuses on two layers: number four, the transport layer, built on standards like TCP and UDP, the physical building blocks of internet data traffic, and number seven, the application layer, built on standards like HTTP and FTP, which are dependent on the application using them, i.e. Internet Explorer, Kazaa, Skype, etc. **It monitors 10 billion bits per second at level four and 2500 million bits per second at level seven. For reference, the 256K DSL line I am using equals .25 million bits per second. So one NarusInsight machine can look at about 39,000 DSL lines at once in great detail.** That is a pretty damn big number. This is some really serious hardware with equally serious software. Which is our next subject.

So what exactly is done to and with this data? That's kind of a grey area, so let's try to find what we can. The starting point is called the **Internet Protocol Detail Record**, which Narus helped found. From that FAQ I just linked to, we learn that

IPDR stands for the **Internet Protocol Detail Record, the name comes from the traditional telecom term CDR (Call Detail Record), used to record information about usage activity within the telecom infrastructure (such as a call completion).**

NDM-U stands for Network Data Management - Usage. It refers to a functional operation within the Telecom Management Forum's Telecom Operations Map. The NDM function collects data from devices and services in a service providers network. Usage refers to the type of data which is the focus of this document.

IPDR.org is the non-profit organization that promotes use of the IPDR NDM-U and other related standards. The principle deliverable for IPDR.org is the NDM-U specification and related development tools.

And is it actually being used?

IPDR.org has been in existence since 1999 and **more than a dozen vendors have actual IPDR implementations "etched in code". Their systems are actually able to talk to each other and interoperate.** Version 2.5 and up of the NDM-U represents a stable basis for development. IPDR.org's Interoperability Pavilion is a working demonstration of multiple companies exchanging service usage data in that format.

Service usage data. That would be data on the actual usage of the Internet. And what kind of data would this be? Way back in 1999, **this article** stated

In an effort to provide more complex network traffic analysis, Narus is introducing its semantic network traffic service. The company cites research which predicts the fast-growing ISP sector will become stagnant without the ability to offer differentiated services. In order to gain significant revenues from these services, a technology was necessary to allow usage based pricing.

"We realized that, at the heart of the data that is needed to accurately measure usage and enable 'pay-as-you-go' business models for Internet service providers, is what we call the 'semantics' of network traffic," said Ori Cohen, Narus' founder and chief executive officer.

"In short, by seeing the 'semantics' of network traffic, service providers can see 'inside' the data, providing much more detailed insight about the use of the Internet and the perceived value of specific applications than existing technologies allow."

Semantic Traffic Analysis uses network technology to **consistently capture and analyze all IP data streams on heavily trafficked networks remotely and non-invasively**. In addition, the semantics of the data stream are determined also, as well as the protocol used and the application taking place. A variety of other data is available as well.

Remember that **semantics** is not just the data, but rather the meaning of the data. It looks at the data in a more comprehensive way than looking for keywords. Each NarusInsight machine does this at 2500 million bits per second, in real-time.

You really wonder why BushCo doesn't want to talk about this stuff? **It's the biggest invasion of privacy in history by several orders of magnitude.**

How can we know? From **Narus' Lawful Intercept and Regulatory Compliance page:**

Explosive Internet growth in recent years has transformed worldwide communications, yielding tremendous efficiencies and benefits, as well as many risks.

For example, terrorist attacks around the globe have been carefully orchestrated through Internet-based forms of communications such as e-mail, messaging, hidden Web pages and now VoIP, forcing governmental organizations and law enforcement agencies to re-evaluate how they are providing public security as it becomes so much easier and faster to communicate electronically.

Recent mandates and the resulting standards referenced under CALEA in the United States and ETSI in Western Europe aim to preserve the right of law enforcement agencies to conduct authorized electronic surveillance in an effort to protect the public and its right to privacy. However, these mandates create IT headaches for carriers as they struggle to meet the requirements.

With a suite of products targeted at meeting lawful intercept requirements, Narus simplifies lawful intercept tasks helping carriers and agencies meet requirements without experiencing any degradation in service quality.

Key benefits

- Packet-mode data intercepts for Service Providers and Carriers.
- Wireline to wireless and WiFi or dialup to broadband.**
- "Instant Compliance" with CALEA and ETSI for simple, fast and hands-free compliance.
- Carrier-grade speeds, performance and scalability.
- Supports all of your services, out-of-the-box.
- Securely manages resources while simplifying audits and reporting.
- Network and vendor agnostic.
- Enables additional application for revenue generation or revenue protection.

This data flows right into **NarusInsight Intercept Suite**, which enables

Packet-level, flow-level, and application-level usage information is captured and analyzed as well as raw user session packets for forensic analysis, surveillance or in satisfying regulatory compliance for lawful intercept.

The Lawful Intercept module offers carriers and service providers compliance with regulatory requirements regarding lawful intercept. The Lawful Intercept module provides an end-to-end solution consisting of Administration, Access and Delivery functions. The Lawful Intercept module is compliant with CALEA and ETSI standards. **It can be seamlessly integrated with third party products for testing/validation or as a complete law enforcement solution.**

The Directed Analysis module seamlessly integrates with NarusInsight Secure Suite or other DDoS, intrusion or anomaly detection systems, securely providing analysts with real-time, surgical targeting of suspect information (from flow to application to full packets). The Directed Analysis module provides industry standard formats and offers tools for archival and integration with third party investigative tools.

These capabilities include playback of streaming media (i.e. VoIP), rendering of web pages, examination of e-mail and the ability to analyze the payload/attachments of e-mail or file transfer protocols. Narus partner products offer the ability to quickly analyze information collected by the Directed Analysis or Lawful Intercept modules. When Narus partners' powerful analytic tools are combined with the surgical targeting and real-time collection capabilities of Directed Analysis and Lawful Intercept modules, analysts or law enforcement agents are provided capabilities that have been unavailable thus far.

Imagine how great a tool "instant compliance" with **the Communications Assistance for Law Enforcement Act** could be with this kind of reach and detail. Especially if a secret Presidential Directive allows it to be used without the warrants required under the Act.

That's what it appears we are up against, folks. Real-time semantic data monitoring on a huge scale. A scale beyond what most of us can even comprehend. It's scary.

Tags: **EFF**, **NSA**, **spying**, **Bush**, **AT&T**, **warrantless wiretaps** (all tags)

[View Comments](#) | 36 comments

China's Internet
censorship

* Timeline: memory of
Tiananmen

* Streaming video (coming
Friday)

[Read More...](#)



I SUPPORT
THE WAR
ON EASTER

" *The God Who Wasn't
There* irreverently lays out
the case that [Jesus Christ](#)

[never existed](#) ." --

Newsweek

"Provocative -- to put it
mildly."

-- **Los Angeles Times**

[Read More...](#)

Reserve Ad!

Classifieds

IMPEACH BUSH!

Magnetic bumper
stickers, T-shirts, fridge
magnets, caps, mugs.
"BE NICE TO AMERICA
OR WE'LL BRING
DEMOCRACY TO YOUR
COUNTRY." "If you're not
outraged, you're not
paying attention." "IRAQ

Reserve your spot!



Support Bloggers' Rights!

Candidates

Netroots Endorsed

[Combined fundraising page](#)

Jon Tester

Senate

Montana

Francine Busby

House

California 50th CD

Ned Lamont

Senate

Connecticut

Eric Massa

House

New York 29th CD



[Daily Kos homepage](#)

© Kos Media, LLC

Site content may be used for any purpose without explicit permission unless otherwise specified.

[Privacy Policy](#)

Powered by [Scoop](#).